IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs. **CR. No. 16-4571 JCH**

GUY ROSENSCHEIN,

Defendant.

MEMORANDUM OPINION AND ORDER

This matter is before the Court on closely related motions to suppress evidence, as well as two supplemental motions, filed by Defendant Guy Rosenschein ("Rosenschein") as described below. On July 27, 2020, the case came before the Court for a five-day evidentiary hearing. In light of the COVID-19 pandemic and over Rosenschein's objection, the Court conducted the hearing via videoconference. The parties provided the Court with paper and electronic copies of their exhibits in advance of the hearing and also displayed them onscreen during the hearing. All witnesses and counsel participated from their homes or offices with the exception of the Defendant, who was present in the courtroom with his two attorneys and their support staff. Having considered the testimony, the exhibits, and the arguments of counsel, the Court concludes that Rosenschein's suppression motions under *Ackerman*, as well as both supplemental motions, should be denied.

The Court will address Rosenschein's *Franks* motions and his motion to suppress for unconstitutional conduct in a separate Memorandum Opinion and Order.

FACTUAL BACKGROUND

Rosenschein is charged with the distribution and possession of child pornography. [See Doc. 1]. Detective Kyle Hartsock of the Bernalillo County Sheriff's Office ("BCSO") began investigating Rosenschein in November of 2016 after his department received two CyberTipline Reports from the National Center for Missing and Exploited Children ("NCMEC"). The two CyberTipline Reports that the BCSO received were generated by Chatstep, an electronic service provider that hosts internet-based conversations between users. Chatstep was able to identify the alleged child pornography through its use of Microsoft's PhotoDNA service. PhotoDNA is a cloud-based service developed by Microsoft to help prevent the sharing of child pornography. It works by analyzing digital images to create a unique "hash value" (consisting of a long string of letters and numbers) for that image that is then matched against databases of hash values of known child pornography. Through its use of PhotoDNA, Chatstep identified, but did not view, two images allegedly distributed by Rosenschein as child pornography before the images were submitted to the NCMEC through the CyberTipline. NCMEC did not view the images either, but it used the IP address attached to the tips to determine the probable physical origin of the images. NCMEC then forwarded the CybperTip reports, including the flagged images, to the New Mexico Attorney General's Office Internet Crimes Against Children Task Force ("ICAC"), which then contacted Detective Hartsock.

PROCEDURAL BACKGROUND

In the first suppression motion, *Motion to Suppress Evidence & Request for an Evidentiary Hearing under Franks v. Delaware* [Doc. 71], Rosenschein asks the Court to suppress all evidence collected from the search of his home, as well as the fruits of all evidence collected from that search. As grounds for his motion, he contends that the search warrant signed by a judge from the

Second Judicial District Court was based on Bernalillo County Sheriff's Office Detective Kyle Hartsock's affidavit, which he alleges contained recklessly misleading information and omitted critical information that undermined the validity of the warrant. In his second motion, *Defendant Dr. Rosenschein's Motion to Suppress Evidence under Ackerman* [Doc. 74], he asserts that NCMEC has been held to be a government agent, and that Microsoft[1], in turn, is acting as NCMEC's agent by designing and providing its PhotoDNA service to electronic communication service providers. Rosenschein's motion turns on several premises: (1) that Microsoft is NCMEC's agent, and therefore is itself a government agent, (2) that PhotoDNA searches and seizes online images when it generates hash values, and (3) that an individual has a reasonable expectation of privacy in images he uploads to Chatstep. Rosenschein's third motion to suppress, *Motion to Suppress Evidence Due to Detective Hartsock's Unconstitutional Conduct* [Doc. 77], asserts the argument that Detective Kyle Hartsock improperly viewed images that Rosenschein uploaded to Chatstep without a warrant, and then sought a warrant to search Rosenschein's home based on viewing those images. Rosenschein contends that Hartsock's affidavit failed to inform the judge that he had viewed the images without a warrant, failed to give a detailed description of the images, and failed to attach the images to his affidavit. Rosenschein contends that without this information, there was no probable cause for the warrant. All three motions were filed in April of 2018.

In May of 2018, the Government filed a combined response to all three motions to suppress. [Doc. 82]. On May 30, 2018, Rosenschein filed his consolidated reply brief. [Doc. 86]. On June 27, 2018, the Government filed a surreply [Doc. 94], and on August 15, 2018, Rosenschein filed a surreply [Doc. 108] to the Government's surreply. Meanwhile, at a status conference on July 17,

[1] As discussed below, Rosenschein later amended his motion to assert that Chatstep is also a government agent.

2018, the parties informed the Court that they would need to litigate various discovery issues before they would be prepared for a hearing on the trio of motions to suppress. They requested that while that discovery and anticipated litigation was pending, the Court move forward on Rosenschein's fourth, unrelated motion to suppress statements.[2]

The Court set the trio of motions to suppress for a joint hearing to begin June 10, 2019 [Doc. 132]. In the meantime, Rosenschein sought discovery from NCMEC, Microsoft, Chatstep, and other third parties, resulting in extensive motion practice, including but not limited to various motions for Rule 17(a) and 17(c) subpoenas, motions to quash, motions to compel, motions to reconsider, motions to intervene by third parties, and motions to exclude witnesses. Due to the pendency of those motions, the Court granted Rosenschein's motion to vacate the June 10, 2019 hearing. The undersigned addressed the bulk of the discovery motions, while two others were referred to a United States Magistrate Judge. Rosenschein filed objections to the Magistrate Judge's recommendations, which then had to be briefed and ruled upon by the undersigned.

Furthermore, the outcome of the discovery litigation prompted the parties to file yet more motions and briefing regarding the three motions to suppress. These include: (1) Rosenschein's *Updated Motion to Suppress Illegally Obtained Evidence for Lack of Probable Cause* [Doc. 254], the Government's response [Doc. 278], *Dr. Rosenschein's Supplemental Brief in Support of His Suppression Motion Under Franks v. Delaware* [Doc. 293], the Government's response [Doc. 295], and Rosenschein's reply [Doc. 299]; and (2) *Defendant Dr. Rosenschein's Corrected,*

[2] Rosenschein's fourth suppression motion [Doc. 61] asked the Court to suppress statements Rosenschein made as a result of interrogation after his arrest. That motion was also fully briefed by this time and ready for hearing. The Court set it for hearing on September 11, 2018. However, on August 30, 2018, the Government filed an unopposed motion to continue the hearing [Doc. 109]. The motion was granted, and the Court reset the evidentiary hearing for November 28, 2018. On February 21, 2019, the Court granted the motion to suppress statements. [Doc. 118].

Amended Motion to Suppress Evidence Under Ackerman [Doc. 269] and the Government's response [Doc. 279].

Over the Defendant's objection, the hearing was reset for July 27, 2020 via video conference. Defendant argued that the hearing should be postponed until such time that it could be held safely with all participants present in the courtroom. The court overruled his objection [Doc. 294], and discovery motion practice continued until shortly before the hearing.

DISCUSSION

I. *Ackerman* Motion

In his original motion [Doc. 74] to suppress evidence under *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), Rosenschein argues that NCMEC has been held to be a government entity and agent, and that Microsoft, in turn, is acting as NCMEC's agent by designing PhotoDNA to search for known images of child pornography and by providing the PhotoDNA service to electronic communication service providers like Chatstep. In his subsequent corrected and amended motion [Doc. 269], Rosenschein argues that both Microsoft and Chatstep acted as government agents for NCMEC by using PhotoDNA to search for images of child pornography and seize his private correspondence, thereby violating his Fourth Amendment right to be free from unreasonable search and seizure of images that he uploaded on Chatstep. He also argues that he had a subjective as well as an objectively reasonable expectation of privacy in those images.

A. Reasonable Expectation of Privacy

1. Legal Standard

"A search for purposes of the Fourth Amendment occurs when government officials violate an individual's legitimate expectation of privacy." *United States v. Nicholson*, 144 F.3d 632, 636 (10th Cir. 1998). If there is no recognizable privacy interest or if the search is performed by a

private actor, then the Fourth Amendment does not apply. The Supreme Court has set out a two-part test for analyzing whether a defendant had a reasonable expectation of privacy in a place to be searched: first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). The defendant carries the burden of making the threshold showing that he has both a subjective expectation and an objectively reasonable expectation of privacy in the area searched and in relation to the items seized." *United States v. Stokes*, 829 F.3d 47, 51 (1st Cir. 2016); *Nicholson*, 144 F.3d at 636.

2. Discussion

(a) Facts

The developers of Chatstep, Saurabh Davala and Sundeep Gottipati, intended to create a website that made it easy for people to communicate or "chat" with each other online without having to create an account. [Davala, Tr. 7/27/2020 at 174-75; Gottipatti, Tr. 7/30/2020 at 12]. The website touted itself as a place for "secure, private beautiful online group chat." Ex. 4. During the relevant time period in this case, Chatstep users were able to use the website's services anonymously, without registering or creating any sort of membership or account. [Davala, Tr. 7/27/2020 at 173, 175; Gottipati, Tr. 7/30/2020 at 12]. The word "secure" on the website referred to the use of "https," which is a secure way for websites to operate, as well as having the option to create a chatroom with a password. [Davala, Tr. 7/27/2020 at 174]. The word "private" on the website referred to that fact, and the fact that users could further hide their identity by choosing any nickname they wanted. [Davala, Tr. 7/27/2020 at 174]. However, from the point of view of Chatstep co-creator Gottipati, Chatstep was never truly private. Rather, it permitted people to

communicate anonymously online, but the developers might still be able to determine someone's identity through their IP address. [Gottipati, Tr. 7/30/2020 at 12-13].

In order to communicate with others on Chatstep, users could click on a link on the homepage to access a list of public chat rooms; in the alternative, they could enter the name of a private chat room and its corresponding password. [Id. at 176, 248]. Thus, a public chat room is one that is available to any anonymous user of the Chatstep website. Conversely, a private chat room is still anonymous but requires a password for entry. [Id. at 175-176]. Finally, the user would enter a nickname that he or she would use while in the chosen chat room. [Id.] Up to 50 users could be in the same chatroom at once. [Id. at 177]. An undercover police officer could join a chat room under a fictional nickname, just like any other user, without any help from Chatstep or its developers. [Id. at 218]. Once in a chatroom, a user could converse or share images with others. [Id. at 177-78].

During the relevant time frame, Chatstep's terms of service (found under the FAQ, or "frequently asked questions" link along the lower left side of any chatroom page) stated, "We may preserve or disclose any information if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; … or to protect Chatstep rights or property." [Id. at 181, 249-250; Exs. 5, 7]. Thus, users of Chatstep were warned that any illegal information or images could be disclosed. [Id.] Around September of 2015, Chatstep also implemented in its chat rooms a "report image" button that, when pressed, would reveal the IP address of the sender of any image. [Davala, Tr. 7/27/2020 at 178-79]. This was meant to act as a deterrent to Chatstep users sharing illegal photos because they would know that other users could report them. [Davala, Tr. 7/28/2020 at 99-100; Gottipati, Tr. 7/30/2020 at 83].

The evidence shows that on July 31 and August 8, 2016, an individual using the pseudonym "Carlo" entered a Chatstep chat room and uploaded images that Chatstep sent to PhotoDNA, which then flagged the images as matching known child pornography. [Exs. 10, 11, 16, 17]. Chatstep did not review the images. [Davala, Tr. 7/27/2020 at 202, 210, 213]. In turn, Chatstep initiated a CyberTipline Report, which PhotoDNA then routed to NCMEC. [Lilleskare, Tr. 7/27/2020 at 41-42]. Due to a data loss by Chatstep's web hosting provider, Chatstep could not independently confirm the information in the receipts they received from the CyberTipline, and there is no evidence as to whether Carlo attempted to share the images in a private or public chat room on Chatstep. [Davala, Tr. 7/27/2020 at 211, 214; Davala, Tr. 7/28/2020 at 90-92; Gottipati, Tr. 7/30/2020 at 104].

In lieu of live testimony, Rosenschein has offered his Declaration [Doc. 86-3, Ex. AM] of May 30, 2018, in which he states, "When using the Chatstep Internet site, I believed that all of my communications, in any form, would remain private."

(b) Analysis

Rosenschein attempts to show that he had a subjective expectation of privacy through his single statement in his declaration that he believed that all of his communications on Chatstep, "in any form, would remain private." He relies, at least in part, on the fact that the website advertised "secure, private beautiful online group chat." However, the Court struggles to find Rosenschein's subjective expectation of privacy credible. Rosenschein admitted that he had used Chatstep multiple times and had used various nicknames—so many, in fact, that he could not remember them all. [Doc. 279-14 at 4 and 8 of 10]. Thus, one can infer that he was quite familiar with Chatstep and the fact that people there did not use their real names. He acknowledged that he didn't know the people he chatted with. [Id. at 4 of 10]. And, given the fact that he was familiar with

Chatstep, one can also infer that he knew about the "report image" button that appeared whenever an image was shared. That button, which was active during the relevant time frame, would put every Chatstep user, including Rosenschein, on notice that anyone could report them, either to Chatstep or to law enforcement, if that user uploaded an illegal image. Those facts significantly undercut Rosenschein's claim to a subjective expectation of privacy.

Regardless of the credibility of his asserted subjective beliefs, Rosenschein has not met his burden to show that he had an objectively reasonable expectation of privacy in the images uploaded to a chatroom on Chatstep. The evidence before the Court shows a user like Rosenschein could not know the identities of those with whom he was sharing images on Chatstep. The website was entirely anonymous, required no registration or identification, and merely asked users to select a nickname that could be changed or altered by the user at will. At any time, a user could be communicating with a law enforcement officer investigating crimes against children or the user's own nextdoor neighbor—there was simply no way to know. Despite these facts, Rosenschein asserts that he expected that his communications would remain private. It strains credulity to think that the law recognizes as private communications made to unknown individuals. As a matter of common sense, the first step one takes in preserving the privacy of a communication is to know the identity of the person with whom one is communicating. The second step is to try to control who has access to the communication. But on Chatstep, users could do neither of these things, as a chat room was essentially a public space that individuals could enter and leave at will. Rosenschein has presented no evidence that the communications at issue in this case took place in a private chatroom, which although it remained anonymous, at least required a password for entry. "Those who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private." *United*

States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007). Essentially, Rosenschein confuses anonymity with privacy, but they are not one in the same.

This case is similar to *United States v. Morel*, 922 F.3d 1, 9-10 (1st Cir. 2019), in which the defendant was charged with possession of child pornography after uploading images to a website which made it impossible to prevent third parties from accessing the images. Although the images in *Morel* were uploaded to albums on the website and therefore publicly available in a more permanent manner than images on Chatstep, *id*. at 10, that case is analogous this one because in both instances, the defendant exercised no control over who viewed the images, and in that sense they were publicly available. The First Circuit concluded that Morel lacked a reasonable expectation of privacy because "[n]o evidence suggests that Morel took affirmative steps to protect the images." *Id*.

Based on similar reasoning, several courts have concluded that users do not have a reasonable expectation of privacy in messages they upload in chat rooms. *See, e.g., United States v. Bode*, 2013 WL 4501303 at *16 (D. Md. Aug. 21, 2013) (unpublished) (distinguishing chatrooms, which are exposed to the public, from emails, which are private, person-to-person communications); *United States v. Maxwell*, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (noting that "[m]essages sent to the public at large in [a] 'chat room' . . . lose any semblance of privacy."). As one district court observed in rejecting a claim of Fourth Amendment protection for messages posted in publicly accessible online chat rooms, the defendant "could not have a reasonable expectation of privacy in the chat rooms," because "when Defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent." *United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997). These courts all examined the public nature of chat

rooms, including the lack of control over and knowledge of who received the communications. All those same criteria are present in this case.

For the same reasons, the Court concludes that Rosenschein lacked a reasonable expectation of privacy under the Fourth Amendment in his communications on Chatstep, including any images he uploaded.

B. Government Agent or Private Actor?

1. Legal Standard

Fourth Amendment protections do not apply to a private search. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Thus, a search by a private citizen is not subject to the strictures of the Fourth Amendment unless that private citizen is acting as a government agent. *Id.* at 113-14 (1984). "[I]n some cases a search by a private citizen may be transformed into a governmental search implicating the Fourth Amendment if the government coerces, dominates or directs the actions of a private person conducting the search or seizure." *United States v. Poe*, 556 F.3d 1113, 1123 (10th Cir. 2009) (quotation omitted). In the Tenth Circuit, a court must look at several factors in determining whether a private citizen was acting as an agent of the government. The first of these is whether the government had knowledge of and acquiesced in the private person's intrusive conduct; the second is whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes. *Id.* The Tenth Circuit has also held that "knowledge and acquiescence . . . encompass the requirement that the government agent must also affirmatively encourage, initiate, or instigate the private action." *United States v. Benoit*, 713 F.3d 1, 9 (10th Cir. 2013).

In addition, the Fourth Amendment does not apply if the government merely replicates a prior private search. *Jacobsen*, 466 U.S. at 115.

The defendant has the burden of showing government action. *United States v. Gumerlock*, 590 F.2d 794, 799 (9th Cir. 1979); *United States v. Freeland*, 562 F.2d 383, 385 (6th Cir. 1977). The controlling standard at a suppression hearing is proof by a preponderance of the evidence. *Nix v. Williams*, 467 U.S. 431, 444 n.5 (1984).

2. Relevant Facts

(a) Microsoft

Microsoft is a large software company that provides software services to a wide array of customers, from consumers to businesses. [Lilleskare, Tr. 7/27/2020 at 20]. Rosenschein called two Microsoft witnesses to testify at the suppression hearing: Courtney Gregoire, in-house counsel who in 2016 was assigned to Microsoft's digital crimes unit [Gregoire, Tr. 7/30/2020 at 108], and Gregory Clark, program manager. [Clark, Tr. 7/30/2020 at 162]. The government called Jeff Lilleskare, who is not a software developer but the manager of Microsoft's online safety and security group. [Lilleskare, Tr. 7/27/2020 at 19]. Finally, Rosenschein called Professor Hany Farid to testify regarding his role in the development of PhotoDNA.

PhotoDNA is a software program that analyzes an image, breaks it down, and using an algorithm creates a unique identifier in the form of a string of letters and/or numbers known as a signature or a "hash" for that image. [Lilleskare, Tr. 7/27/2020 at 28-29]. That unique identifier can then be compared to a database of unique identifiers of known child pornography images. Unlike previous hash-matching technology, PhotoDNA can match images even if they have been altered in some way, such as cropped or turned black and white. [Lilleskare, Tr. 7/27/2020 at 30-31, 73; Shehan, Tr. 7/29/2020 at 83-84]. This makes PhotoDNA harder to circumvent than earlier hashing technology. [[Lilleskare, Tr. 7/27/2020 at 31]. PhotoDNA's rate of false positives is "very rare." [Lilleskare, Tr. 7/27/2020 at 31-33, 154-55]. Occasionally, an image is mischaracterized as

child pornography when it is not. [*Id*. at 107]. Several different groups, including NCMEC, a U.S. industry group, and a couple of groups from Canada contributed their databases of known child pornography to be used by PhotoDNA as a standard set against which to match potentially illegal images. NCMEC did not direct Microsoft to use its database. [Lilleskare, Tr. 7/27/2020 at 38, 90]. NCMEC hosts the database and limits access to only registered companies, but it does not contribute information to it or review its contents. [Id. at 90-91].

Lilleskare's group focused on online safety work, the purpose of which was to protect customers from exposure to online harm, including child sexual abuse material. [Lilleskare, Tr. 7/27/2020 at 21-22]. Microsoft's desire to create PhotoDNA was rooted in its business interests. [Gregoire, Tr. 7/30/2020 at 151]. Keeping child pornography off the internet generally, and Microsoft's services specifically, served to protect Microsoft's brand image, as well as to help keep the broader world of the internet safe for consumers. [Lilleskare, Tr. 7/27/2020 at 22, 50; Gregoire, Tr. 7/30/2020 at 152, 156-158]. This serves Microsoft's business interests because if people see the internet as dangerous, they are less likely to use and buy Microsoft's products. [Lilleskare, Tr. 7/27/2020 at 23, 156, 158]. Further, PhotoDNA helps to protect Microsoft employees from having to review images of child sexual exploitation that are reported to Microsoft by its customers. [Gregoire, Tr. 7/30/2020 at 151-52].

PhotoDNA is part of Microsoft's effort to protect its customers and its brand. [Lilleskare, Tr. 7/27/2020 at 22]. Microsoft developed PhotoDNA in partnership with Dartmouth College and Professor Hany Farid. [Id. at 24; Shehan, Tr 7/29/2020 at 81]. Neither NCMEC nor any law enforcement agency was involved in the design or development of PhotoDNA. [Lilleskare, Tr. 7/27/2020 at 25; Farid, Tr. 7/31/2020 at 41; Shehan, Tr. 7/29/2020 at 81-82]. After PhotoDNA was designed and developed, Microsoft granted a limited license to NCMEC for the purpose of

testing the code and creating a set of reference hashes from its existing database of known images of child pornography. [Lilleskare, Tr. 7/27/2020 at 25-26; Gregoire, Tr. 7/30/2020 at 113, 126, 153; Shehan, Tr 7/29/2020 at 82, 85]. After the testing was complete, Microsoft donated a license to NCMEC to use PhotoDNA to further NCMEC's mission of fighting child pornography online. [Shehan, Tr 7/29/2020 at 152]. In an article written by Ms. Gregoire, she stated: "None of our PhotoDNA work could happen without partnership from industry leaders and advocates. We especially rely on partnerships with [NCMEC] and the International Center for Missing and Exploited Children (ICMEC) to ensure that PhotoDNA evolves to meet new and changing needs in the fight against exploitation material." [Ex. AL].

Later, Microsoft went on to develop the PhotoDNA cloud service, which gives the ability to computer program developers and other third parties to subscribe to the PhotoDNA technology on "the cloud" and incorporate it into their products. [Lilleskare, Tr. 7/27/2020 at 26-27]. NCMEC was not involved in the development of the PhotoDNA cloud service. [Id. at 26]. Microsoft uses PhotoDNA on its own products, but rather than using it via the cloud, it uses an on-premises version. [Lilleskare, Tr. 7/27/2020 at 27].

The PhotoDNA cloud service has two separate components: the hash matching service, and the reporting service that allows the ESP to make an automated CyberTipline report to NCMEC in the event of a match. [Lilleskare, Tr. 7/27/2020 at 40-41]. The reporting service is optional. [Id. at 40]. When an ESP uses PhotoDNA to make a report, the ESP is the entity that is submitting the report to the CyberTipline, while Microsoft routes the report on behalf of the ESP. [Lilleskare, Tr. 7/27/2020 at 41].

Microsoft makes the PhotoDNA cloud service available without charge to qualified companies. [Lilleskare, Tr. 7/27/2020 at 63]. Microsoft also makes certain tools, such as free

forensic and image review, available to law enforcement through PhotoDNA. [Id. at 67]. PhotoDNA provides NCMEC with aggregate reports summarizing the number of images matched to previously known hashes or signatures of child pornography images, and customers who use PhotoDNA must consent to that. [Lilleskare, Tr. 7/27/2020 at 76, 78].

Since the inception of PhotoDNA, Microsoft has tried to improve upon it. [Gregoire, Tr. 7/30/2020 at 147-48]. As the technology improves, Microsoft and any other user of PhotoDNA continue to have a legal obligation to report to NCMEC any image of child sexual exploitation. [Id. at 148].

(b) NCMEC

NCMEC has operated the CyberTipline since 1998. [Shehan, Tr. 7/29/2020 at 58]. It is a centralized mechanism for reporting suspected child sexual exploitation. [Id.]. Someone making a report to the CyberTipline must include the incident type and the date/time of the incident; all other information associated with the incident, including the name, email address, IP address, web address, screen name, is voluntary. [Id. at 60-62]. Electronic service providers can send information to NCMEC, but NCMEC has no way to unilaterally access information stored by ESPs. [Id. at 62]. If the CyberTip contains an IP address, NCMEC runs an automated search on a public website to find a physical location associated with that address. [Id. at 68]. Depending on what other information the reporting person or entity has included in the CyberTip, NCMEC may conduct other open source searches. [Id. at 68-69]. However, NCMEC does not open any files included with the report unless the reporting party indicates that they have already opened it. [Id. at 70]. Finally, NCMEC makes the report accessible to law enforcement through a virtual private network. [Id. at 71].

(c) Chatstep

Chatstep was founded by Saurabh Davala and Sundeep Gottipati in July of 2012. [Davala, Tr. 7/27/2020 at 236; Gottipati, Tr. 7/30/2020 at 11]. Both men credibly testified that it was in their business interest to report and eliminate illegal content like child pornography on their website. [Davala, Tr. 7/27/2020 at 216-17, 219; Gottipati, Tr. 7/30/2020 at 88]. They wanted to stay in the good graces of their advertisers, as that was their primary revenue source. [Davala, Tr. 7/27/2020 at 183, 216]. And, they felt that child pornography on the website would ruin Chatstep's reputation and turn away not only advertisers, but also many users, thereby adversely affecting their revenue. [Davala, Tr. 7/27/2020 at 183; Davala, Tr. 7/28/2020 at 100; Gottipati, Tr. 7/30/2020 at 79-80]. Finally, Chatstep had been receiving emailed reports from users complaining of child pornography on the website. [Davala, Tr. 7/27/2020 at 184]. As a result, the Chatstep developers became concerned. They tried several approaches to combat child pornography on their site, including banning certain types of room names, nicknames, and IP addresses. [Id. at 203-04; Davala, Tr. 7/28/2020 at 100; Gottipati, Tr. 7/30/2020 at 37-38].

In July of 2014, Chatstep received an email from Maryann Caden at NCMEC. [Ex. 8; Ex. A0001]. Through that email, the developers learned of their legal duty as an electronic service provider to report images of child pornography on their service that they learn about. [Id.; Davala, Tr. 7/27/2020 at 185; Gottipati, Tr. 7/30/2020 at 85]. The email states:

> NCMEC has created a separate, secure website specifically for electronic service providers to comply with 18 USC § 2258A. The secure site allows ESPs to upload any content related to the reported incident to the CyberTipline. When a company submits a report, they will receive a receipt, should they ever need to prove compliance with 18 USC § 2258A. I've attached a copy of the reporting law for your reference.

[Ex. 8] The developers saw the email as "guidance" and felt that while it was not legally required, Chatstep should go forward with obtaining credentials for the CyberTipline. [Ex. 8 at 2; Davala,

Tr. 7/27/2020 at 187; Gottipati, 7/30/2020 at 86]. Because Mr. Davala and Mr. Gottipati were busy with school and viewed the instances of illegal images as "one-offs," they felt no particular sense of urgency and did not sign up with the CyberTipline until ten months later, in May of 2015. [Davala, Tr. 7/27/2020 at 190; Gottipati, Tr. 7/30/2020 at 15-16, 87]. By then, the number of incidents of child pornography being uploaded on Chatstep had risen, and they began to take NCMEC's request more seriously. [Gottipati, Tr. 7/30/2020 at 16]. During those months, they viewed the follow-up emails they received from NCMEC as reminders, not as coercion or pressure to sign up. [Davala, Tr. 7/27/2020 at 190-91, 193].

Eventually, the developers decided to move forward with the NCMEC reporting system because it would help their business. [Gottipati, Tr. 7/30/2020 at 87]. However, the CyberTipline system was a manual reporting system. [Gottipati, Tr. 7/30/2020 at 15]. Davala wanted to have something like PhotoDNA running on the Chatstep website because it would automate the process of finding and reporting child pornography, thereby eliminating the need for Chatstep to manually review images that were reported by users. [Davala, Tr. 7/27/2020 at 193-94, 198, 217; Gottipati, Tr. 7/30/2020 at 19-20]. It could also be programmed to automatically fill in fields on the CyberTipline reports, a task that would be too time-consuming and tedious to do by hand. [Gottipati, Tr. 7/30/2020 at 18-19]. They found PhotoDNA through a simple web search and without any input or direction from either NCMEC, law enforcement, or Microsoft. [Davala, Tr. 7/27/2020 at 194; Gottipati, Tr. 7/30/2020 at 20, 89].

In the summer of 2015 Chatstep's initial application to Microsoft to use PhotoDNA was not successful, but after forming a limited liability company the developers tried again and were able to register it in April or May of 2016. [Davala, Tr. 7/27/2020 at 195]. Initially, there were some technical problems incorporating PhotoDNA into Chatstep's platform. However, Gottipati

communicated with individuals from both NCMEC and Microsoft to solve those issues because he thought it was in Chatstep's best interest to get PhotoDNA working. [Gottipati, Tr. 7/30/2020 at 90-91].

Once operational on Chatstep's platform, PhotoDNA scanned every uploaded image. When a Chatstep user uploaded an image, Chatstep would temporarily "hold on to that image and pass it over to PhotoDNA." [Davala, Tr. 7/27/2020 at 198]. If PhotoDNA did not recognize it as a match, Chatstep released and shared the image to everyone in the chat room. [Id. at 198-99]. On the other hand, if PhotoDNA made a match to known child pornography, Chatstep recorded the nickname and IP address of the sender in an automated report and told PhotoDNA to forward the report to NCMEC. [Id. at 199, 201-02]. In the case of a match, the uploading user received a generic user error but was not informed of the specific reason. [Id.] That way, users would not be able to "test" the system to learn which images they could successfully upload and which ones they could not. [Id. at 200]. This was done, at least in part, at Microsoft's recommendation. [Clark, Tr. at 7/30/2020 at 177, 184]. Davala testified that if he felt that PhotoDNA had not helped his business, he would have looked for an alternative way to accomplish the same automated scanning and reporting. [Davala, Tr. 7/27/2020 at 218]. And, even if Chatstep had not been required by law to report suspected child pornography to NCMEC, the developers would still have wanted to use it in order to further their business interest and keep that type of content off of Chatstep. [Id. at 203; Gottipati, Tr. 7/30/2020 at 88].

On one occasion, in late June of 2016, Chatstep received notice that an image of a woman wearing a BestBuy shirt had been attached to a CyberTip report sent to law enforcement in Nebraska. The image contained no pornography. [Ex. A at 195]. Clark testified that this type of "mismatch" was not something that he saw often. [Clark, Tr. 7/30/3030 at 174]. It was not a

problem with PhotoDNA, but rather with Chatstep's reporting system. [Clark, Tr. 7/30/2020 at 183].

On different occasions, Chatstep has cooperated with law enforcement investigating alleged child pornography on the website. [Davala, Tr. 7/27/2020 at 219]. For example, in 2015 they received a request for information from a French (or possibly Canadian) policeman who asked for information about a Chatstep user accused of sharing illegal content. [Davala, Tr. 7/27/2020 at 205, 245; Gottipati, Tr. 7/30/2020 at 26]. After that, Davala and Gottipati thought that they should start keeping and storing searchable room entry logs so that they could more easily respond to information requests from law enforcement. This was a voluntary act that would save the developers time and help them to clean up Chatstep. [Davala, Tr. 7/27/2020 at 205-206, 245; Gottipati, Tr. 7/30/2020 at 26-27, 92]. The room entry logs contained the name of the room, nicknames of persons entering the room, IP address, date, and time, but not the substance of the communications shared. [Davala, Tr. 7/28/2020 at 103; Gottipati, Tr. 7/30/2020 at 94]. This same information was available to any Chatstep user in a particular room. [Id.]

Soon after that, the Chatstep developers were contacted by an agent working for the Department of Homeland Security asking them what sort of data they stored. [Davala, Tr. 7/27/2020 at 191; Gottipati Tr. 7/30/2020 at 27; Ex. A0008]. Gottipati told the agent about the room entry logs they had created, and without prompting offered him a username and password to enable him to search the logs. [Ex. A0009]. Gottipati did this so that Chatstep could avoid the work of addressing individual subpoenas for information from law enforcement. [Gottipati, Tr. 7/30/2020 at 29-30, 92-93, 95]. The developers created the logs because it was in their business interest to get child pornography off their website and because they hoped that law enforcement could help them do that; the developers were not coerced. [Davala, Tr. 7/27/2020 at 205-06, 219;

Davala, Tr. 7/28/2020 at 101-102, 104; Gottipati, Tr. 7/30/2020 at 30-32]. Thereafter, other law enforcement officers began contacting them, and Gottipati was responsive. [Gottipati, Tr. 7/30/2020 at 38-40, 45-46]. However, they never communicated with Detective Hartsock or the Bernalillo County Sheriff's department, the law enforcement agency investigating this case. [Gottipati, Tr. 7/30/2020 at 99-100]. Finally, the developers prioritized their business interest over helping law enforcement. [Gottipati, Tr. 7/30/2020 at 97-98].

3. Analysis

The Court concludes that neither Microsoft nor Chatstep is a government agent. Both were private entities with regard to their actions in this case.

When a statute or regulation compels a private party to conduct a search, the private party acts as an agent of the government. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989). The *Ackerman* court relied in large measure on a federal statutory scheme to conclude that NCMEC is both a governmental entity and a government agent because the law compels NCMEC in a variety of ways. "NCMEC's two primary authorizing statutes—18 U.S.C. § 2258A and 42 U.S.C. § 5773(b)—mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person." *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016). NCMEC is statutorily required to maintain the CyberTipline, to forward reports to law enforcement, and to receive child pornography and review its contents. In contrast, those statutory requirements do not apply to private electronic service providers ("ESPs") like Microsoft and Chatstep. Unlike NCMEC, which is identified as the recipient of Cybertip reports, electronic service providers like Microsoft and Chatstep have the discretion to monitor their traffic or not. The statute explicitly disclaims a scanning or monitoring requirement for ESPs,

18 U.S.C. § 2258A(f), and mandates only reporting of apparent images of child pornography that they are aware of, § 2258A(a). In fact, ESPs "might just as well take steps to avoid discovering reportable information" to avoid penalties for failure to report. *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010). The statutory scheme here does not support a conclusion that either Microsoft or Chatstep is a government agent.

Thus, the question is whether the government had knowledge of and acquiesced in Chatstep and Microsoft's intrusive conduct, and whether Chatstep's developers intended to assist law enforcement agents or instead acted to further their own purposes.

(a) Chatstep

In its initial years, the founders of Chatstep did not install PhotoDNA or otherwise screen the contents of the photographs shared by their customers. They violated no law in not doing so. Chatstep was subject to mandatory reporting if they learned of child pornography, but without monitoring software in place, they saw and reported nothing. It was only after customers complained that they decided to take steps to eradicate child pornography from their site. Increasing inquiries from law enforcement agencies also contributed to their decision. After installing PhotoDNA, they became subject to mandatory reporting requirements, which they satisfied through an automated link to the CyberTipline.

The evidence at the suppression hearing demonstrated that the second prong of the test for government agency is not satisfied—that is, Chatstep is not a government agent because the developers decided to monitor their customer traffic for child pornography for business reasons and not to satisfy or assist the government or law enforcement. They were concerned that the proliferation of child pornography on their site would hurt Chatstep's reputation, drive away advertisers, and discourage legitimate customers. On the other hand, they needed an automated

mechanism for finding and reporting illicit material in order to save valuable time. For these reasons, Chatstep decided to use PhotoDNA. There is no evidence that Chatstep received any payment from the government concerning Cybertips or that they had a law enforcement presence at their location to assist with these issues. For Fourth Amendment purposes, Chatstep and its developers are private actors, not representatives of government.

The fact that Chatstep's business interest aligned with the government's interest in pursuing purveyors of child pornography is of no moment. The Tenth Circuit has held that, "[w]e do not inquire if the police benefitted from the private conduct, but if the [private actor] had a 'legitimate, independent motivation' to conduct the search." *United States v. Poe*, 556 F.3d 1113, 1124 (10th Cir. 2009) (quoting *United States v. Smythe*, 84 F.3d 1240, 1243 (10th Cir. 1996)). Thus, the *Poe* court concluded that bounty hunters, who were motivated by financial reward, were not government agents even though their goal of apprehending the defendant aligned with that of law enforcement. *Id*. This rationale extends into situations such as this, where electronic service providers are motivated to remove child pornography from their services in order to advance their business interests. "Sharing a goal with the Government is insufficient to transform AOL from a private actor into a Government agent; a private party becomes a state actor for Fourth Amendment purposes only when it is motivated *solely or primarily* by a desire to assist or aid law enforcement in an investigation." *United States v. Stevenson*, 2012 WL 12895560 at *3 (S.D. Iowa June 20, 2012), *aff'd* , 727 F.3d 825 (8th Cir. 2013). Similarly, in *United States v. Miller*, 2017 WL 2705963 at *4 (E.D. Ky. Jun. 23, 2017) (unpublished), the court concluded that Google was not a government agent despite its collaborative relationship with NCMEC and the fact that it shared the government's goal of eliminating child pornography from the internet. The court relied on

evidence that "[r]idding [its] products and services of child abuse images is critically important to protecting [Google's] users, product, brand, and business interests." *Id*.

Similarly, the government offered credible evidence that Chatstep and its developers had legitimate, overarching business reasons for monitoring their website and reporting suspected child pornography. Thus, Chatstep had a legitimate, independent business motivation to conduct the search. Rosenschein has not met his burden to prove that Chatstep was a government agent.

(b) Microsoft

For the same reasons, the Court reaches a similar conclusion with regard to Microsoft. Unlike NCMEC, Microsoft is not statutorily required to proactively seek out child exploitation or to protect children online—only to report to NCMEC if the company becomes aware of it. There is no evidence to support the conclusion that Microsoft was coerced or pressured into developing PhotoDNA. There is no evidence that the government played a significant role in the research and development of PhotoDNA, or that it used any pressure to induce or instigate Microsoft to develop or implement it. After it was developed, NCMEC did test PhotoDNA for Microsoft. However, that collaboration did not turn Microsoft into a government agent. Rather, as several witnesses testified, Microsoft's development of PhotoDNA was in furtherance of its own business interest in keeping the internet and the online community free of child pornography. As a computer and internet-based company, protecting consumer confidence in online platforms is in Microsoft's best interests so that consumers will be willing to use Microsoft's products.

Notably, other courts have declined to find that ESPs like Microsoft are government agents when they search for child pornography on their platforms. Like Rosenschein does here, the defendant in *Miller* argued that Google's "'close relationship and collaborative crime fighting efforts' with NCMEC" turned it into a government agency. *Miller*, 2017 WL 2705963 at *2.

However, the court concluded that ESPs who "voluntarily [search] for child pornography and report apparent child pornography to NCMEC" are not government agents because the statutory reporting requirements are not enough to transform them into such, and because there was no evidence that NCMEC imposes burdens on the ESP that the statute does not. *Id.* at *3. The court also relied on Google's business interest in avoiding losing users through association to abusive content and conduct, *id*. at *4, the same business interest that motivated Microsoft in this case. Other courts have reached similar conclusions. *See, e.g., United States v. Coyne*, 387 F. Supp. 3d 387, 396 (D. Vt. 2018) (concluding that neither Microsoft nor Chatstep was a government agent); *United States v. Wilson*, 2017 WL 2733879 at *10 (S.D. Ca. Jun. 26, 2017) (unpublished) (concluding that Google's extensive screening process constituted a private search of defendant's email account); *United States v. Rosenow*, 2018 WL 6064949 at *8 (S.D. Cal. Nov. 20, 2018) (unpublished) (concluding that in searching user accounts, Yahoo acted in a private capacity "in compliance with internal policies, business interests, and all existing laws").

The Court concludes that in designing, testing, and making PhotoDNA available to others, Microsoft was acting as a private entity. Rosenschein has not met his burden to show that it was a government agent in this case.

(c) Private Search

Having concluded that neither Microsoft nor Chatstep was a government agent in this case, the Court must now turn to the question of whether Agent Hartsock expanded their private search.

It is well established that a government actor does not violate the Fourth Amendment by replicating a search done by a private individual. *United States v. Jacobsen*, 466 U.S. 109, 116 (1984). The Fourth Amendment is only implicated if the government exceeds the scope of the prior search done by a private individual. *Id*. "Under the private search doctrine, the critical

measures of whether a governmental search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it re-examines the evidence and, relatedly, how certain it is regarding what it will find." *United States v. Lichtenberger*, 786 F.3d 478, 485-86 (6th Cir. 2015) (citing *Jacobsen*, 466 U.S. at 119-20). With respect to child pornography, the Sixth Circuit has held that a government search does not exceed the scope of the private search and therefore was permissible when "the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband," " 'learn[ed] nothing that had not previously been learned during the private search,' and 'infringed no legitimate expectation of privacy.'" *Id.* (alteration in original) (quoting *United States v. Bowers*, 594 F.3d 522, 526 (6th Cir. 2010)).

Here, the Court has determined that both Chatstep and Microsoft are private entities. Further, it has determined that Chatstep used PhotoDNA, a Microsoft product, to run a hash of the relevant images and compare them to known images of child pornography. Finally, the evidence shows that no human at Chatstep, Microsoft, or NCMEC opened and viewed the images before the CyberTips were forwarded to Detective Hartsock and he opened them. Therefore, the Court must determine whether those images were "searched" before they reached Detective Hartsock. If so, the Court must then decide whether Detective Hartsock exceeded the scope of that search by opening and viewing the images.

As to the first question, the evidence in this case shows that PhotoDNA automatically scanned the uploaded images to create a hash, and then compared each of those hashes against a database of hashes of known images of child pornography. PhotoDNA alerted Chatstep to each match, and Chatstep generated CyberTips, which PhotoDNA forwarded to NCMEC. After receiving the two CyberTips, NCMEC (a government agent under *Ackerman*) did not view the

images in question but merely forwarded the tips to law enforcement, who were then able to retrieve the images themselves through a virtual private network. [Shehan, Tr. 7/29/2020 at 69-72, 95-96, 101; Ex. 10 at 6 of 7; Ex. 11 at 6 of 7]. Rosenchein does not assert otherwise. Further, the parties agree that a hash match does constitute a search. [Doc. 269 at 45-46; Doc. 279 at 39]. Therefore, the Court concludes that there was a prior, private search of the images.

The second question is whether Agent Hartsock exceeded the scope of Chatstep's private search by looking at the images. The testimony shows that the hash values in the comparison database were taken from images that were either previously viewed by ESPs or that were already publicly available, and which were then subsequently viewed by at least two NCMEC employees to make sure that they qualify as images of child exploitation. The hash values for those images were then added to NCMEC's database before July of 2016. [Shehan, Tr. 7/29/2020 at 75-76; 102-05]. In addition, the evidence showed that PhotoDNA is highly reliable. Under these facts, the Court concludes that Detective Hartsock did not exceed the scope of the earlier private search. This is because the government had relatively little information to gain when Detective Hartsock opened those images, and it was nearly certain that when he did, he would find child pornography. As previously discussed, these images were examined by several other individuals prior to being found to be child pornography and placed into the NCMEC database. Furthermore, the evidence at the hearing shows that while PhotoDNA is not infallible, mismatches, or "false positives," are very rare.

In very similar circumstances[3], the Fifth Circuit has held that the police did not exceed the scope of the earlier private search when the officer opened an image that had already been

[3] In contrast, this case is very dissimilar from *United States v. Ackernman*, 831 F.3d 1292 (10th Cir. 2016), in which NCMEC opened not only the images that had been flagged by AOL's hash matching program, but also opened additional unflagged images and the defendant's email

identified as apparent child pornography by Microsoft PhotoDNA. *United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018). In *Reddick*, the defendant uploaded digital images to Microsoft SkyDrive, a cloud hosting service. PhotoDNA hashed those images and, upon comparing them to a database of known images of child pornography, found a match. *Id.* at 637-38. Microsoft then sent a CyberTip to NCMEC, which forwarded the information to law enforcement— who, in turn, opened the files and confirmed that they contained child pornography. *Id*. at 638. The *Reddick* court rejected the argument that this constituted an unlawful warrantless search. In doing so, it relied on the Supreme Court's decision in *Jacobsen*, 466 U.S. 109, in which FedEx employees opened a package and discovered a white powder. They called the Drug Enforcement Administration, which conducted field tests and determined that the substance was cocaine. *Id*. at 111. The Supreme Court held that by opening the package, the FedEx employees had already frustrated the defendant's expectation of privacy in its contents: "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* at 117.

According to the Fifth Circuit in *Reddick*, a similar frustration of the defendant's privacy interests occurred when PhotoDNA automatically reviewed the hash values of the images he uploaded and compared them against a database of hash values of known child pornography. *Reddick*, 900 F.3d at 639. Expanding on that concept, the Fifth Circuit reasoned that due to the reliability of hash matching, when the detective opened Reddick's files he already knew that they were images of child pornography whose hashes matched those of images in the NCMEC database. *Id*. Further, his visual inspection of the images was like the chemical field tests in *Jacobsen*—it

---

messages, which had not been previously opened by AOL. No such expansion of the private search took place in this case.

"merely dispelled any residual doubt about the contents of the files." *Id*. Stated another way, the officer's visual review of the suspected images enabled the police "to learn nothing that had not previously been learned during the private search." *Jacobsen*, 466 U.S. at 120. Therefore, there was no violation of the Fourth Amendment.

Like in *Reddick*, Detective Hartsock's opening of the images forwarded by Chatstep in this case was akin to the chemical tests in *Jacobsen*. Detective Hartsock already knew that the two images he opened had been electronically matched with previously identified child pornography; there was very little to learn from merely confirming their contents by opening them. Thus, his warrantless search was within the scope of the earlier private search Chatstep performed.

Because Detective Hartsock did not exceed the scope of the private search, the motion to suppress will be denied.

C. Good Faith

The Government argues that even if Rosenschein had a reasonable expectation of privacy in images he uploaded to Chatstep, and even if Chatstep or Microsoft was a government agent that performed a warrantless search, then the evidence still should be suppressed because Detective Hartsock acted in good faith when he viewed those images. However, having found that Rosenschein did not meet his burden to show that he had a reasonable expectation of privacy or that Chatstep and Microsoft were government agents or that Detective Hartsock exceeded the scope of the private search, the Court will not reach the question of whether the good faith exception to the Fourth Amendment applies.

II. Other Motions

A. Rosenschein's Motion to Dismiss, or in the Alternative, to Compel [Doc. 277]

In his motion, Rosenschein asserts that various entities in this case—Chatstep, Microsoft, and NCMEC—have conspired to destroy or withhold evidence in a bid to frame him for possessing and uploading images that he never possessed. In his motion, Rosenschein "demands the production of the computer software so Dr. Rosenschein can demonstrate unequivocally for the Court what reports should have been produced to the defense but never were . . ." [Doc. 277].

During the suppression hearing, the Court heard extensive oral argument from counsel regarding this motion. [Tr. 7/29/2020]. For the reasons stated on the record, the Court denied the motion in open court. Accordingly, Defendant's motion to dismiss or to compel discovery is denied.

B. Rosenschein's Motion to Take Judicial Notice [Doc. 303]

1. Background

After the suppression hearing was already underway, Rosenschein filed a motion asking the Court to take judicial notice of Defendant's Exhibit AD, which appears to have three components[4] relating to a civil case from Washington state court. In that civil case, the plaintiff claimed that his work on Microsoft's online safety team reviewing digital content for terms of use violations, including child pornography, caused him to develop post-traumatic stress disorder. The three documents at issue are transcripts of the Rule 30(b)(6) depositions of Microsoft employees Suzanne Kinzer and Robert Sizemore in *Soto v. Microsoft Corporation*, No. 16-2-31049-4 SEA (Wash. Sup. Ct.), and an undated "Policy Overview" document purportedly written by Robert

[4] Also included is a declaration from Soto's attorney certifying that the deposition transcripts and Policy Overview are true and correct copies.

Sizemore. All three together were marked as Defendant's Exhibit AD at the suppression hearing. Based on the included excerpt from Sizemore's deposition, the Policy Overview document appears to have been drafted by Robert Sizemore. He testified that he reviewed a large quantity of documents given to him by others and synthesized them into the Policy Overview. It appears he wrote it in preparation for litigation, and it is attached as an exhibit to his deposition. There is no clear relevance of the Kinzer deposition transcript to either the Policy Overview or the Sizemore deposition.

The defense focuses on statements in the Policy Overview relating to changes in how Microsoft addressed child sexual abuse material on its private services. On July 27, 2020, defense counsel raised the "Policy Overview" document during cross examination of Mr. Lilleskare, asking him why a Microsoft policy was changed or adopted. Counsel for Microsoft objected on grounds of attorney-client privilege, and the Government objected on relevance. [Tr. 7/27/2020 at 129-148]. When Mr. Lilleskare was asked whether he was familiar with the document, he stated that he had never seen it before. [Id. at 143]. Ultimately, the Court sustained Microsoft's objection on relevance grounds but allowed the defense to file a written motion on judicial notice. [Id. at 146-47].

On July 29, 2020, defense counsel argued that the "Policy Overview" was relevant to Microsoft's status as a government agent by showing that Microsoft intended to assist law enforcement. The Court denied Rosenschein's request to admit the documents on relevance grounds but permitted him to submit a proffer on the issue of judicial notice. [Tr. 7/29/2020 at 213-14, 217-18, 220].

2. Arguments of counsel

Rosenschein argues that the Court should take judicial notice of Exhibit AD as previous testimony and exhibits from a related court proceeding under *Anderson v. Cramlet*, 789 F.2d 840, 845 (10th Cir. 1986). He contends that the "documents discuss the internal decision of Microsoft to change their application of PhotoDNA in light of possible Fourth Amendment limitations on their actions, demonstrating a clear acknowledgement of both Microsoft's understanding of its actions as an agent of law enforcement and Microsoft's intent to continue assisting law enforcement by preserving evidence for prosecution of criminal cases." [Doc. 303 at 4].

In response, the Government argues that the documents in question are subject to reasonable dispute, making them inappropriate for judicial notice.

3. Analysis

Rule 201(b)(2) of the Federal Rules of Evidence states that that "[t]he court may judicially notice a fact that is not subject to reasonable dispute because it . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Under Rule 201(c), [t]he court must take judicial notice if a party requests it and the court is supplied with the necessary information." Federal courts may take judicial notice of proceedings that are relevant to the matter at hand. *See, e.g., Kowalski v. Gagne*, 914 F.2d 299, 305-06 (1st Cir. 1990); *Ctr. for Native Ecosystems v. United States Fish & Wildlife Serv*., 795 F. Supp. 2d 1199, 1205-06 (D. Colo. 2011) (declining to take judicial notice of a fact with attenuated relevance to the case).

Here, the Court declines to take judicial notice for three reasons. First, as the Court already explained on the record at the hearing, the document is not relevant because it speaks to Microsoft's actions in dealing with child sexual exploitation on its *private* services and servers. In contrast, this case is about whether Microsoft is a government agent with respect to its development and licensing of PhotoDNA cloud services for the public, including ESPs like Chatstep. Second,

the Court concludes that judicial notice is not appropriate for the same reasons set forth in the Government's response brief. [Doc. 306]. The Court will not repeat those arguments here. Third, in this instance judicial notice would be futile because even if the Court considered the document, it would not change the ruling regarding whether Microsoft is a government agent. Although Rosenschein focuses on statements in the document that speak to assisting law enforcement or decreasing the risk of the exclusion of evidence in criminal prosecutions, the document also sets forth the various reasons its policy changes serve Microsoft's business interests. Specifically, the Policy Overview discusses the reasons why Microsoft reduced or stopped scanning its private servers for child sexual exploitation materials. Throughout, the document sets forth legitimate business reasons for Microsoft's change in policy: "to reduce the risk a customer's account was shut down in error," recognizing "a customer's expectations of privacy in their private folders," "fight[ing] actual CSAM [child sexual abuse material]" (which this Court has already recognized as something that Microsoft would do to promote its business); making the project "scalable [] with increasing use of cloud storage." Finally, to protect its employees: "Microsoft determined that to protect its customers and scale the business in a manageable way for Microsoft employees and vendors, it would cease actively scanning private folders in OneDrive while continuing to scan public folders and images shared from private folders to others. . . . the effect of these policy changes was to reduce the amount of employee and vendor exposure to CSAM and other graphic or disturbing content." The effect of this evidence is to support the conclusion that while law enforcement may have benefitted from Microsoft's policies, those policies served Microsoft's business interests. The mere fact that a company's business interests align with those of law enforcement does not transform that business into a government agent.

Accordingly, the motion for judicial notice will be denied.

IT IS THEREFORE ORDERED that:

(1) *Defendant Dr. Rosenschein's Motion to Suppress Evidence under Ackerman* [Doc. 74] and *Defendant Dr. Rosenschein's Corrected, Amended Motion to Suppress Evidence Under Ackerman* [Doc. 269] are **DENIED**;

(2) Rosenschein's Motion to Dismiss, or in the Alternative, to Compel [Doc. 277] is **DENIED;**

(3) Rosenschein's Motion to Take Judicial Notice [Doc. 303] is **DENIED**.

SENIOR UNITED STATES DISTRICT JUDGE